DECLARATION

I, Jun Inohara, a national of Japan, c/o Shoyo Intellectual Property Firm, Tobu Yokohama 2nd Bldg. 6F, 15-1, Kitasaiwai 2-chome, Nishi-ku, Yokohama-shi, Kanagawa-ken, Japan, declare that I am familiar with both the English and Japanese languages, that I am the translator of the attached document, that to the best of my knowledge and belief the attached document is a true and accurate translation of Japanese Patent Application No. 2003-154870 filed on May 30, 2003, and further that these statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Dated this 27 day of November, 2007

Signature

Jun Inohara

Jun Inohara

Japanese Patent Application No. 2003-154870

【Document name】 Patent application

【Reference Number】 HK15005000

【Filing date】 May 30, 2003

【Directed to】 Commissioner of the Patent Office

【International Patent Classification】 G06F 12/00

【Inventor 】

(Address) System Development Laboratory, Hitachi Ltd., 1099 Ouzenji, Aso-ku, Kawasaki-shi, Kanagawa-ken, Japan

(Name) Kenichi Shimooka

【Inventor 】

(Address) System Development Laboratory, Hitachi Ltd., 1099 Ouzenji, Aso-ku, Kawasaki-shi, Kanagawa-ken, Japan

(Name) Masaharu Asano

【Applicant for the Patent Application】

(Applicant's Registration Number) 000005108

(Name) Hitachi Ltd.,

【Agent】

(Agent's Registration Number) 100084032

(Patent Attorney)

(Name) Iwao Mishina

(Telephone No) 045-316-3711

【Indication of Official Fee】

(Registration Number for Payment in advance) 011992

2003-154870

(Amount of payment) 21000

【List of the attached document】

(Document) Specification 1

(Document) Drawing 1

(Document) Abstract 1

【Is Proof Necessity】 Yes

【Document】 Specification

【Title of the Invention】

DATA PROTECTING APPARATUS AND METHOD, AND COMPUTER SYSTEM

【Scope of the Claims】

【Claim 1】 A data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, and a storage control unit for controlling communication between said computer and said storage volume, wherein said data protection apparatus comprises:

an event detection unit for detecting an event occurrence; and

a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit detects an event.

【Claim 2】 A data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, a storage control unit for controlling communication between said computer and said storage volume, and an illegal intrusion detection unit for detecting an illegal intrusion against said computer, wherein said data protection apparatus comprises:

an event detection unit for receiving the detection of the illegal intrusion from said illegal intrusion detection unit; and

a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit receives the detection of the illegal intrusion.

【Claim 3】 A data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, a storage control unit for controlling communication between said computer and said storage volume, and a computer virus detection unit for detecting a computer virus in said storage volume, wherein said data protection apparatus comprises:

an event detection unit for receiving the detection of the computer virus from said computer virus detection unit; and

a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit receives the detection of said computer virus.

【Claim 4】 A data protection method for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, and a storage control unit for controlling communication between said computer and said storage volume, wherein said data protection method comprises steps of:

detecting an event occurrence; and

instructing said storage control unit to stop communication between said computer and said storage volume, when said event is detected.

【Claim 5】 A program for making an information processing apparatus perform data protection of a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, and a storage control unit for controlling communication between said computer and said storage volume, wherein said program makes said information processing apparatus perform processes of:

detecting an event occurrence; and

instructing said storage control unit to stop communication between said computer and said storage volume, after said event is detected.

【Claim 6】 A computer system comprising a storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, a storage control unit for controlling communication between said computer and said storage volume, and a data protection apparatus for protecting data in said storage volume, wherein:

said data protection apparatus comprises:

an event detection unit for detecting an event occurrence; and

a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit detects an event.

【Claim 7】 A data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned

for storing data duplicated from said storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said data protection apparatus comprises:

an event detection unit for detecting an event occurrence; and

a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event.

【Claim8】 A data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, a computer for reading and writing data from and to said storage volume, a storage control unit for controlling data transfer from said storage volume to said replicated volume, and an illegal intrusion detection unit for detecting an illegal intrusion into said computer wherein said data protection apparatus comprises:

an event detection unit for receiving the detection of the illegal intrusion from said illegal intrusion detection unit; and

a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume.

【Claim9】 A data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, a storage control unit for controlling data transfer from said storage volume to said replicated volume,

and a computer virus detection unit for detecting a computer virus in said storage wherein said data protection apparatus comprises:

an event detection unit for receiving the detection of the computer virus from said computer virus detection unit; and

a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume.

【Claim10】 A data protection method for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said data protection method comprises steps of:

detecting an event occurrence; and

instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event is detected.

【Claim11】 A program for making an information processing apparatus perform data protection of a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said program makes said information processing apparatus perform processes of:

detecting an event occurrence; and

instructing said storage control unit to stop data transfer from said

storage volume to said replicated volume, when said event is detected.

【Claim12】 A storage medium that stores the program according to Claim 5 or Claim 11 and can be read by the information processing apparatus.

【Claim13】 A computer system comprising a storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, a storage control unit for controlling data transfer from said storage volume to said replicated volume, and a data protection apparatus for protecting data in said storage volume, wherein:

said data protection apparatus comprises:

an event detection unit for detecting an event occurrence; and

a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event.

【Claim14】 A computer system according to Claim 13, wherein:

write data to said storage volume is transferred by said storage control unit to said replicated volume with a delay of a given time.

【Claim15】 A computer system according to Claim 13, wherein:

as said replicated volume, a plurality of replicated volumes are provided; and

said storage control unit switches a transfer destination of write data of said storage volume, at given time intervals among said plurality of replicated volumes.

【Claim16】 A computer system according to Claim 15, wherein:

said computer system further comprises an alteration detection unit that reads given data in said plurality of replicated volumes to detect respective differences between the given data; and

the event detected by said event detection unit is a detection result of the differences between the given data, with said detection result being received from said alteration detection unit.

【Claim17】 A computer system according to Claim 16, wherein:

said computer system further comprises a computer for reading and writing data from and to said storage volume;

said storage control unit further controls communication between said computer and said storage volume; and

said data protection apparatus instructs said storage controller to stop communication between said computer and said storage when said event detection unit detects said event.

【Detailed Description of the Invention】

【0001】

【Technical Field of the Invention】

The present invention relates to a technique of protecting data in a computer system at the time of detecting an computer fraud against the computer system.

【0002】

【Prior Art】

Recently, as computer networks become popular, service businesses using computer systems, such as electric commerce, are flourishing. On the other

hand, damage such as data destruction, data leakage, data alteration and the like owing to illegal intrusion into a computer system, a computer virus, or the like (hereinafter, these are generically referred to as computer fraud(s)) becomes serious problems. There is the possibility that transaction information held on a computer system is lost by data destruction or the like owing to these computer frauds, causing tremendous losses. As a result of this, confidence in a company that operates the computer system may be lost. Further, generally speaking, large costs and much time are required to recover damaged data. Thus, it is very important to protect data against computer frauds.

【0003】

As countermeasures against computer frauds, prevention should be mentioned first. Conventionally, computer frauds on a computer system have been prevented by installation of a firewall between the computer system and an external network, user authentication using a one-time password, setting of ACL (Access Control List) defining files/programs accessible by each user, and the like. However, techniques of computer frauds are developed and diversified day by day, and thus, as a matter of fact, it is impossible to prevent computer frauds perfectly.

【0004】

Accordingly, by way of precaution against unprevented intrusion, monitoring and an ex post facto countermeasure become important. As conventionally-known typical monitoring means, may be mentioned IDS (Intrusion Detection System) for coping with illegal intrusion, virus detection software for coping with computer viruses.

【0005】

IDS monitors illegal intrusion and the like by monitoring a log file and analyzing port scan, for example. When an illegal intrusion or the like is detected, a session with an intruder is disconnected, or a front-end switches existing between an intruded computer system and an external network is operated to disconnect the path from the intruder. Further, virus detection software detects computer viruses by performing pattern matching between file contents and code patterns of computer viruses, for example. When a computer virus is detected, an infected file is deleted, or a virus pattern is erased. Details of these techniques are described in non-patent document 1, for example.

【0006】

【Non-patent document 1】

Foundation for Multimedia Communications, Network Management Section, "Introduction to Network Management for Beginners", 6.3.3. Intrusion Detection System, [online], May 15, 2002 (found on December 19, 2002) on the Internet <URL:http//www.fmmc.or.jp/~fm/nwmg/manage/main.html>.

【0007】

【Problems that the Invention is to Solve】

Generally speaking, IDS requires a certain period of time for detecting an illegal intrusion from its occurrence. Sometimes, an intruder uses this time to put a Trojan horse or to open a backdoor for the next intrusion. Here, the Trojan horse means a disguised program that gives rise to a destructive action or causes infection with a computer virus once the program is executed being taken as a harmless program.

【0008】

In these cases, it is not possible to sufficiently protect data in a

computer system by the above-mentioned disconnection of a session or disconnection of a path at the front end. This is because there is a possibility that an authorized user activates the Trojan horse without knowing it, or the intruder intrudes again by entering through the backdoor to pass through the IDS.

【0009】

Further, in the case of infection with a self-propagating computer virus that infects other files or programs one after another, even when a virus detection software detects and deletes the computer virus, the infection may spread before other files or the like are inspected.

【0010】

Thus, an object of the present invention is to protect data in a computer system when an computer fraud against the computer system is detected.

【0011】

【Means of Solving the Problems】

To attain the object, a first mode of the present invention provides a data protection apparatus for protecting data in a storage volume in a computer system comprising said storage volume assigned for storing data, a computer for reading and writing data from and to said storage volume, and a storage control unit for controlling communication between said computer and said storage volume, wherein said data protection apparatus comprises an event detection unit for detecting occurrence of an event, and a path disconnection unit for instructing said storage control unit to stop communication between said computer and said storage volume, when said event detection unit detects an event.

【0012】

As an event whose occurrence is to be detected, can be mentioned an computer fraud detected by an intrusion detection unit or a virus detection unit.

【0013】

According to the present mode, when an computer fraud is detected, it is possible to protect data by disconnecting a back-end path between the computer suffering from the computer fraud and its storage volume.

【0014】

Further to attain the above object, a second mode of the present invention provides a data protection apparatus for protecting data in a storage volume in a computer system, with said computer system comprising said storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from said storage volume, and a storage control unit for controlling data transfer from said storage volume to said replicated volume, wherein said data protection apparatus comprises: an event detection unit for detecting occurrence of an event; and a replication stopping unit for instructing said storage control unit to stop data transfer from said storage volume to said replicated volume, when said event detection unit detects an event.

【0015】

The storage control unit may transfer write data of the storage volume to said replicated volume with a delay of a given time. Or, a plurality of replicated volumes may be provided so that the storage control unit may switch a transfer destination of write data of the storage volume, at given time intervals among the plurality of replicated volumes.

【0016】

According to the present mode, it is possible to secure data replication before occurrence of an computer fraud.

【0017】

【Preferred Embodiments】

[First Embodiment]

Fig. 1 is a block diagram showing a system configuration of a first embodiment of the present invention.

【0018】

A system of the first embodiment comprises a front-end switch 30, a host 40, a back-end switch 50, a storage 60, and a data protection apparatus 70, and is connected to a network 20.

【0019】

Although the data protection apparatus 70 is described in the present and other embodiments as one independent apparatus, the data protection apparatus 70 may be provided inside the host 40 or built in the switch 30. Further, although the switch 50 also is described as one independent apparatus in the present and other embodiments, the switch 50 may be provided inside the host 40 or the storage 60. Further, although the storage 60 also is described as one and independent apparatus in the present and other embodiments, the storage 60 may be provided in the host 40. Further, although the relation between the host 40 and the data protection apparatus 70 is illustrated as a one-to-one relation in Fig. 1 and other figures, the relation may be a many-to-one relation. Further, although the relation between the host 40 and the storage 60 is illustrated also as a one-to-one relation in Fig. 1, the relation may be one-to-many, many-to-one, or many-to-many.

【0020】

A computer 10 connected to the network 20 is used as a terminal for using the service provided by the host 40. However, a cracker may use the computer 10 to perform an computer fraud against the host 40. As the computer 10, a PC (Personal Computer) or a portable information terminal may be mentioned, for example. Although only one computer 10 is illustrated in Fig. 1 and other figures, a plurality of the computers 10 may exist.

【0021】

The network 20 may be Internet using IP (Internet Protocol), LAN (Local Area Network), WAN (Wide Area Network), or SAN (Storage volume Network) using FC (Fiber Channel), for example.

【0022】

The front-end switch 30 controls a connection between the network 20 and the host 40. However, in the present and other embodiments, it is possible that the switch 30 does not exist and the network 20 and the host 40 are connected directly.

【0023】

The host 40 provides services such as electric commerce and video streaming to the computer 10 through the network 20. However, the host 40 is not limited to a host that provides services, and may be a host that manages internal data without providing services to the outside. The host 40 comprises: a port 41 functioning as an interface with the front-end switch 30; a storage volume 42 storing an intrusion detection program 43 for detecting an illegal access and a virus detection software 44 for detecting computer viruses; a memory 45; a processor 46; a port 47 functioning as an interface

with the back-end switch 50; and a port 48 functioning as an interface with the data protection apparatus 70.

【0024】

It is described in the present and other embodiments that the intrusion detection program 43, the virus detection software 44, and the like are stored in the storage volume 42 provided in the host 40. However, the intrusion detection program 43, the virus detection software 44 and the like may be stored in the storage 60, the data protection apparatus 70, a storage volume of another computer, or a storage medium. In these cases, the host 40 can dispense with the storage volume 42. Further, it is favorable that both the intrusion detection program 43 and the virus detection software 44 exist. However, either the intrusion detection program 43 or the virus detection software 44 may not exist. Further, although Fig. 1 and other figures illustrates one port 41 and one port 47, a plurality of ports 41 and a plurality of ports 47 may exist.

【0025】

The storage 60 is a storage provided with a storage volume 64 for storing data to be protected. The storage volume 64 stores, for example, programs for providing services to the computer 10, and other data. Further, the storage 60 comprises: a port 61 which is an interface with the switch 50 for sending and receiving data; an SVP (Service Processor) 62 which is an interface for acquiring and setting configuration information; and a controller 63 for controlling the connection between the port 61 and the storage volume 64 based on the configuration information set by the SVP 62. Although Fig. 1 illustrates one port 61 and one storage volume 64, a plurality of ports 61 and a plurality of storage volumes 64 may exist.

【0026】

The data protection apparatus 70 is an apparatus characteristic of the present invention, and comprises: a port 71 functioning as an interface with the host 40; a storage volume 72; a memory 75; and a processor 76. The storage volume 72 stores an computer fraud receiving program 73 for receiving computer fraud detection results of a below-mentioned intrusion detection unit 43x and a virus detection unit 44x and a data protection program 74 for performing processes of disconnecting a path between the host 40 and the storage volume 64 used by the host 40. The computer fraud receiving program 73 and the data protection program 74 may be stored in another computer, a storage or a storage medium. In that case, the storage volume 72 can be omitted. The data protection apparatus 70 can be composed as a dedicated apparatus, or composed, for example, by a general information processing apparatus such as a PC.

【0027】

Next, will be described operation in the system of the present embodiment.

【0028】

The host 40 loads a program for providing service onto the memory 45, and the processor 46 executes the program. The above-mentioned program reads or writes data from or to the storage volume 64 through the port 47, the back-end switch 50, and the port 61 and controller 63 of the storage 60, in response to a request from the computer 10, or at regular intervals, or on a occasion of occurrence of a certain event, and provides the service to the computer 10 through the port 41, the front-end switch 30 and the network 20.

【0029】

At the same time, the intrusion detection program 43 and the virus detection software 44 are loaded onto the memory 45 and executed by the processor 46. As a result, the intrusion detection unit 43x (not shown) and the virus detection unit 44x (not shown) are virtually realized in the host 40, and these units 43x and 44x monitor whether the host 40 suffers from an computer fraud or the like. Here, the intrusion detection program 43 and the virus detection software 44 may be loaded onto the memory of the data protection apparatus 70 or a memory on another computer, to monitor the host 40 through a network.

【0030】

Further, the computer fraud receiving program 73 in the data protection apparatus 70 is loaded onto the memory 75 and executed by the processor 76. As a result, an computer fraud receiving unit 73x (not shown) is virtually realized in the data protection apparatus 70, to await a notice of detection of an computer fraud. Here, the computer fraud receiving unit 73x may actively monitor whether the intrusion detection unit 43x or the virus detection unit 44x has detected an computer fraud. In that case, for security of the data protection apparatus 70 itself, it is favorable to assure that access from the data protection apparatus 70 to another apparatus is permitted while access from another apparatus such as the host 40 to the data protection apparatus 70 is not permitted.

【0031】

Fig. 2 is a sequence diagram showing a flow from occurrence of an computer fraud against the host 40 to data protection process in the storage volume 64.

【0032】

A cracker (intruder) uses the computer 10 to illegally intrude into the host 40 or to send a computer virus to the host 40 (S101).

【0033】

When the intrusion detection unit 43x detects an illegal intrusion into the host 40 (S103), then the intrusion detection unit 43x notifies the computer fraud receiving unit 73x of the illegal intrusion, through the ports 48 and 71 (S104). Further, similarly when the virus detection unit 44x detects a computer virus, then the virus detection unit 44x notifies the computer fraud receiving unit 43x of the computer virus detection, through the ports 48 and 71.

【0034】

Receiving the detection of the computer fraud against the host 40, the computer fraud receiving unit 73x loads the data protection program 74 onto the memory 75, and makes the processor 76 execute the program 74 (S105). As a result, a data protection unit 74x (not shown) is virtually realized in the data protection apparatus 70. Here, the data protection program 74 may be loaded onto the memory 75 in advance.

【0035】

The data protection unit 74x instructs the switch 50 or the SVP 62 through the port 71 to change the configuration so as to disconnect a back-end path between the host 40 and the storage volume 64 (S106).

【0036】

Consequently, even when a Trojan horse is planted in the storage volume 64 or the like before the intrusion detection unit 43x detects the illegal intrusion, the back-end path between the host 40 and the storage volume 64 is disconnected. Thus, even when the Trojan horse tries to alter data in the

storage volume 64 (S107), the host 40 can not access the storage volume 64 and the alteration ends in a failure (S108).

【0037】

Thus, according to the present embodiment, it is possible to prevent data destruction that may be resulted from an illegal intrusion or its planted fraud.

【0038】

Further, even when an intruder opens a backdoor for the next intrusion before the intrusion detection unit 43x detects an illegal intrusion, the back-end path between the host 40 and the storage volume 64 is disconnected at the time of next intrusion, and thus, the data in the storage volume 64 can not be accessed either.

【0039】

In the case where a self-propagating computer virus is planted in the storage volume 64, there is a possibility that another file has been infected at a point of time when the virus detection unit 44x detects the computer virus. However, the data protection program 74 disconnects the path between the host 40 and the storage volume 64, and accordingly, the infected file can not be loaded onto the memory 45 and executed (i.e., can not activate). In other words, it is possible to protect the data in the storage volume 64 from further infection (destruction).

【0040】

Next, will be described a method of disconnecting the back-end path in S106. Although the present invention is not limited with respect to a method of disconnecting the back-end path, it is possible to mention a method of using zoning of the switch 50, a method of using path configuration

management for the storage 60, and a method of using ACL of the storage 60, for example. The data protection unit 74x may perform one of these methods, or perform a combination of these methods.

【0041】

First, will be described the method of using zoning of the switch 50. Zoning is a function that a switch permits communication between specific ports only. For example, when a zone consists of ports *a*, *b* and *c*, this switch controls communication so that the port *b* can communicate with the ports *a* and *c* but can not communicate with a port *d*.

【0042】

Fig. 3 is a diagram showing an example of a zoning table 100 held by the switch 50 in the present embodiment.

【0043】

A zone ID 101 is a value for identifying a zone uniquely in the switch 50. Although Fig. 3 expresses a zone ID 101 as a number, it is possible to use a character string.

【0044】

A port ID list 102 is a list of port IDs of ports constituting a zone. A port ID is a value for identifying a port uniquely. As a port ID, a port name or a WWN (World Wide Name) may be used, for example.

【0045】

The data protection unit 74x instructs the switch 50 through the port 71 to delete the port 47 from all the port ID list 102 of the zoning table 100. Here, when a port ID list 102 has only one port, the whole zone may be deleted.

【0046】

For example, when the port 47 is the port a, in the example of Fig. 3, the data protection unit 74x makes the zone ID 1 consist of ports b and c only.

【0047】

As a result, the port 47 can not access any storage 60, and accordingly, the data in the storage volume 64 can be protected.

【0048】

Next, will be described the method of using path configuration management for the storage 60, as the method of disconnecting the back-end path.

【0049】

Path configuration management is a function of managing correspondence between storage volume IDs seen from the host and storage volume IDs inside a storage. The host can not access a storage volume that is not set with such correspondence.

【0050】

Fig. 4 is a diagram showing an example of a path configuration table 110 held by the controller 63 in the present embodiment.

【0051】

An internal port ID 111 is an ID for identifying a port 61 uniquely inside the storage 60. A host LUN (Logical Unit Number) 112 is an ID of a storage volume 64 seen from the host 40. An internal LUN 113 is an ID for identifying a storage volume 64 uniquely inside the storage 60.

【0052】

In the example of Fig. 4, when the host 40 tries to access the first storage through the port A, the host 40 accesses the storage volume 64 whose internal LUN is 156.

【0053】

Although a host LUN 112 and an internal LUN 113 are expressed by numbers in Fig. 4, each may be expressed by a character string.

【0054】

The data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to delete any item corresponding to the storage volume 64 used by the host 40 from the path configuration table 110. To know any item corresponding to the storage volume 64, the intrusion detection unit 43x or the virus detection unit 44x sends information on the internal port ID 111 of the port 61 and the host LUN 112 of the storage volume 64 used by the host 40, at the same time when the intrusion detection unit 43x or the virus detection unit 44x notifies the computer fraud receiving unit 73x of detection of an computer fraud. The data protection unit 74x receives the above-mentioned information from the computer fraud receiving unit 73x, and requests the controller 63 to delete the items corresponding to the above-mentioned information from the path configuration table 110. In the case where the storage volume 64 used by the host 40 does not change at the time of operation, a system administrator of the present embodiment may give information on the host 40 and the internal LUN 113 of the storage volume 64 to the data protection unit 74x in advance. An input device such as a keyboard or a mouse of the data protection apparatus 70 is used to set the information through a UI (User Interface) provided by the data protection unit 74x. In this case, when the computer fraud receiving unit 73x detects an computer fraud against the host 40, the data protection unit 74x uses the information to request the controller 63 to delete all the items corresponding to the internal LUN 113 of the storage volume 64 from the path configuration

table 110.

【0055】

For example, when the internal LUN 113 of the storage volume 64 used by the host 40 is 156, the data protection unit 74x deletes items in the first and fourth lines in the example of Fig. 4.

【0056】

As a result, the storage volume 64 can not be accessed from any host 40. Thus, the data in the storage volume 64 is protected.

【0057】

Next, will be described the method of using ACL as the method of disconnecting the back-end path.

【0058】

ACL of a storage means a function that, for each storage volume, only access from specific hosts is permitted.

【0059】

Fig. 5 is a diagram showing an example of an ACL table 120 held by the controller 63 in the present embodiment.

【0060】

An internal port ID 121 is an ID for identifying a port 61 uniquely in the storage 60. A host LUN 122 is an ID of a storage volume seen from the host 40. Here, instead of a host LUN, may be used an internal LUN, which is an ID for identifying a storage volume 64 uniquely in the storage 60. A host port ID list 123 is a list of port IDs of ports 47 that can use a path expressed by a port ID 121 and a host LUN 122. Namely, in the case of Figs. 4 and 5, the ports *a*, *b* and *c* on the side of the host can access the storage volume 64 whose internal LUN is 15 through the port A on the side of the storage, while

the ports *d* and *e* can not.

【0061】

The data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to delete the port 47 from all the host port ID list 123 in the ACL table 120. Here, in the case where a host port ID list 123 includes no port, that item itself can be deleted.

【0062】

For example, assuming that the port 47 is the port *a*, the data protection unit 74x deletes the port *a* from the first and second lines in the example of Fig. 5.

【0063】

As a result, the port 47 can not access any storage volume 64. Thus, the data in the storage volume 64 can be protected.

【0064】

"The method of using zoning of the switch 50" and "the method of using ACL of the storage 60" have the equal effect, while "the method of using path configuration management for the storage 60" has slightly different effects. In the former two methods, only the host 40 suffering from an computer fraud becomes unable to access the storage volume 64, while in the latter method, all hosts become unable to access the storage volume 64. Namely, when one of the former methods is employed, a host that does not suffer from an computer fraud can access the storage volume 64 without interruption, and can continue to provide service. Thus, it is favorable that the data protection unit 74x employs one of the former methods in the case where a plurality of hosts share the storage volume 64 and obviously the data of the storage volume 64 has not been altered and intruded by a computer

virus, and employs the latter method in the other cases.

【0065】

As described above, in the present embodiment, when the intrusion detection unit 43x or the virus detection unit 44x detects an computer fraud, the data protection unit 74x disconnects the back-end path between the host 40 and the storage volume 64. As a result, even if a Trojan horse is planted or a backdoor is opened or an infection with a computer virus occurs before the intrusion detection unit 43x or the virus detection unit 44x detects the computer fraud, it is possible to protect the storage volume 64. This is because the storage volume 64 can not be accessed even when the host 40 tries to acquire data, and, on the other hand, a computer virus existing in the storage volume 64 can not be loaded onto the memory 45 and executed by the processor 46.

[Second Embodiment]

Fig. 6 is a block diagram showing a system configuration of a second embodiment of the present invention.

【0066】

A system of the second embodiment comprises a front-end switch 30, a host 40, a back-end switch 50, storages 60a and 60b, and a data protection apparatus 70, and is connected to a network 20. Further, a computer 10 is connected to the network 20.

【0067】

The computer 10, the network 20, the front-end switch 30, the host 40, and the back-end switch 50 may respectively have the same configuration and function as the first embodiment.

【0068】

In comparison with the storage 60 of the first embodiment, the storage 60a further comprises a port 64a as an interface with the storage 60b, and a transfer delay unit 66 for delaying data reflection from the storage volume 64 onto a replicated volume 67 for a certain period of time.

【0069】

In comparison with the storage 60 of the first embodiment, the storage 60b further comprises a port 65b as an interface with the storage 60a, and the replicated volume 67 for holding data duplicated from the storage volume 64.

【0070】

Although, in the present embodiment, the transfer delay unit 66 is described as one implemented inside the controller 63a, the transfer delay unit 66 may be provided inside the controller 63b or may be provided as an independent apparatus between the port 65a and the port 65b. Further, although, in the present embodiment, each of the storages 60a and 60b is described as an independent apparatus, the storages 60a and 60b may be a single storage. In other words, the storage volume 64 and the replicated volume 67 may exist in the same single storage. Further, although only one replicated volume 67 is described in the present embodiment, a plurality of replicated volumes may exist. Further, each of the ports 65a and 65b is described as one port, however, there may exist a plurality of ports 65a and a plurality of ports 65b.

【0071】

The configuration of the data protection apparatus 70 is similar to the first embodiment. However, a data protection unit 74x, which is virtually realized when a processor 76 executes a data protection program 74, further has a function of stopping data reflection from the storage volume 64 onto the

replicated volume 67, in addition to the functions of the first embodiment.

【0072】

Operation in the system of the present embodiment is fundamentally similar to that of the first embodiment. However, the present embodiment is different from the first embodiment in that the replicated volume 67 for holding data duplicated from the storage volume 64 is set in advance, and the transfer delay unit 66 is set so that data reflection from the storage volume 64 onto the replicated volume 67 is delayed by ΔT. As a result, in a regular operation, the replicated volume 67 always holds data of the storage volume 64 of ΔT time before.

【0073】

Next, will be described a flow from occurrence of an computer fraud against the host 40 to protection of data in the storage volume 64 in the system of the present embodiment. Operation is similar to the first embodiment until the data protection unit 74x instructs the switch 50 or the SVP 62a to change the configuration so as to disconnect the back-end path between the host 40 and the storage volume 64. In addition to this operation, in the present embodiment, the data protection unit 74x instructs the controller 63a or the controller 63b through the port 71 and the SVP 62a or the SVP 62b to cancel or temporarily stop the replication relation (data reflection) between the storage volume 64 and the replicated volume 67.

【0074】

As a result, in comparison with the first embodiment, the present embodiment can further secure data, which was held in the storage volume 64 ΔT time before an computer fraud against the host 40 is detected in the replicated volume 67.

【0075】

Here, to attain an object of securing data held in the storage volume 64 ΔT time before an computer fraud against the host 40 is detected, it is sufficient to cancel or temporarily stop the replication relation (data reflection) between the storage volume 64 and the replicated volume 67. And, it is not necessary to disconnect the back-end path between the host 40 and the storage volume 64.

【0076】

When it is assumed that the intrusion detection unit 43x and the virus detection unit 44x can detect an computer fraud in less than T1 at worst from the time of occurrence of the computer fraud, by setting ΔT time to satisfy $\Delta T \geq T1$, it is secured that the data is stored in the replicated volume 67 before the occurrence of an computer fraud. Accordingly, even if data held in the storage volume 64 is damaged, the system can be restored rapidly by using data stored in the replicated volume 67.

[Third Embodiment]

Fig. 7 is a block diagram showing a system configuration of a third embodiment.

【0077】

A system of the third embodiment comprises a front-end switch 30, a host 40, a back-end switch 50, a storage 60, and a data protection apparatus 70, and is connected to a network 20. Further, a computer 10 is connected to the network 20.

【0078】

The computer 10, the network 20, the front-end switch 30, the host 40, and the back-end switch 50 may each have the same configuration and

function as the first embodiment.

【0079】

In addition to the first embodiment, the storage 60 further comprises replicated volumes 67a – 67c, which are areas for storing data duplicated from the storage volume 64. Although, in the present embodiment, a plurality of storage volumes 67a – 67c are provided in the same storage 60 as the storage volume 64, the storage volumes 67a ~ 67c may be provided in another storage, as shown in the second embodiment. Further, although three replicated volumes exist in the present embodiment, any number of replicated volumes may exist as far as there exist a plurality of storage volumes.

【0080】

A configuration of the data protection apparatus 70 is similar to the second embodiment. However, a data protection unit 74x, which is virtually realized when a processor 76 executes a data protection program 74, further has a function of switching among replicated volumes 67a – 67c, onto which data of the storage volume 64 is reflected, sequentially and periodically at $\Delta T'$ intervals, in addition to the functions of the second embodiment.

【0081】

Operation in the system of the present embodiment is fundamentally same as the first embodiment. However, the present embodiment is different from the first embodiment in that the replicated volumes 67a – 67c for holding data duplicated from the storage volume 64 are set in advance. Further, it is different that the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 at $\Delta T'$ intervals to switch the replicated volume onto which data of the storage volume 64 is reflected.

【0082】

Fig. 8 is a sequence diagram showing a flow of switching among the replicated volumes 67a – 67c onto which data of the storage volume 64 is reflected in the present embodiment.

【0083】

The data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to reflect data of the storage volume 64 onto the replicated volume 67a (S201). Next, after the period of ΔT' (S202), the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to temporarily stop the replication relation between the storage volume 64 and the replicated volume 67a and to reflect data of the storage volume 64 onto the replicated volume 67b (S203). Further, after the period of ΔT' (S204), the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to temporarily stop the replication relation between the storage volume 64 and the replicated volume 67b and to reflect data of the storage volume 64 onto the replicated volume 67c (S205).

【0084】

Further, after the period of ΔT' (S206), the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to temporarily stop the replication relation between the storage volume 64 and the replicated volume 67c (S207), and to reflect data of the storage volume 64 onto the replicated volume 67a (S201). Repeating these processes, the data protection unit 74x switches, at ΔT' intervals, among replicated volumes 67a – 67c, onto which data of storage volume 64 is reflected. Here, the controller 63 may perform the processing of switching, at ΔT' intervals, the replicated volume onto which data of the storage volume 64 is reflected.

【0085】

As described above, in a regular operation, the replicated volumes 67a – 67c hold respective snapshots of the storage volume 64 with ΔT' time differences.

【0086】

Some storages can hold a number of replications of the storage volume 64 by limiting the number of replicated volumes onto which data of the storage volume can be directly reflected, and by reflecting data of the above-mentioned replicated volumes onto another plurality of replicated volumes respectively (cascade connection).

【0087】

Fig. 9 is a diagram showing an example of a relation between a storage volume and replicated volumes in the case of cascade connection.

【0088】

A replicated volume 67A is a replication destination of the storage volume 64 and, at the same time, a replication source of replicated volumes 67Aa and 67Ab. In the same way, a replicated volume 67B is a replication destination of the storage volume 64 and, at the same time, replication source of replicated volumes 67Ba and 67Bb.

【0089】

With respect to a storage having the above-described configuration, the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to reflect data in the storage volume 64 onto the replicated volume 67A and to reflect data in the replicated volume 67A onto the replicated volume 67Aa. Next, after the period of ΔT', the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to temporarily stop the replication relation between the replicated volume 67A and the

replicated volume 67Aa, and to reflect data in the replicated volume 67A onto the replicated volume 67Ab. Further, after the period of ΔT', the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to temporarily stop the replication relation between the replicated volume 67A and replicated volume 67Ab and the replication relation between the storage volume 64 and the replicated volume 67A, and to reflect data in the storage volume 64 onto the replicated volume 67B and data in the replicated volume 67B onto the replicated volume 67Bb. Further, after the period of ΔT', the data protection unit 74x instructs the controller 63 through the port 71 and the SVP 62 to temporarily stop the replication relation between the replicated volume 67B and the replicated volume 67Ba, and to reflect data in the replicated volume 67B onto the replicated volume 67Bb. Repeating these processes, the data protection unit 74x can make the replicated volumes 67Aa, 67Ab, 67Ba and 67Bb, which are located on end nodes, but not replication sources of other replicated volumes, hold respective snapshots of the storage volume 64 at ΔT' time intervals.

【0090】

In the present embodiment, a flow from occurrence of an computer fraud against the host 40 to protection of data in the storage volume 64 is similar to the second embodiment. However, replication relations to all the replicated volumes 67 are stopped.

【0091】

As described above, in comparison with the first embodiment, the present embodiment is effective in that further N-number replicated volumes can hold snapshots of the storage volume 64 at ΔT' time intervals. In the example of Fig. 7, N is three.

【0092】

Here, to attain the object of securing data existing before an occurrence of an computer fraud against the host 40, it is sufficient to cancel or temporarily stop replication relations (data reflection) of the storage volume with all the replicated volumes 67. And, it is not necessary to disconnect the back-end path between the host 40 and the storage volume 64.

【0093】

Assuming that the intrusion detection unit 43x and the virus detection unit 44x can detect an computer fraud in less than T1 at worst from the time of the occurrence of the computer fraud, by setting $\Delta T'$ to satisfy $\Delta T' \geq T1/(N-2)$, it is assured that at least one replicated volume 67 holds data existing before the occurrence of an computer fraud. This is because, even in the worst case where an computer fraud is detected just after a replicated volume onto which data in the storage volume is reflected is switched, the N-number replicated volumes 67 respectively hold data in the storage volume 64 of zero time ago (the present replication destination), zero time ago (the replication destination just before the present one), $\Delta T'$ time ago, ..., and $(N-2)\Delta T'$ time ago. In other words, if $\Delta T' \geq T1/(N-2)$ is satisfied, the data of $(N-2)\Delta T'$ time ago is older than the data of T1 time ago, which means the detected computer fraud occurred after the point of time of T1 time ago. Thus, at least one of the N-number replicated volumes 67 holds the data in the storage volume 64 of $(N-2)\Delta T'$ time ago, which is the data that existed before the occurrence of the computer fraud. As a result, even if data in the storage volume 64 is damaged, the system can be restored rapidly by using data stored in one of the replicated volumes 67.

【0094】

Further, analyzing a log file after detection of an computer fraud, it may be possible to definitely know the time when data in the storage volume 64 began to be destructed or the time when the computer fraud started. In the present embodiment, it is possible to secure the newest data before the mentioned time, namely, data as of T1/(N – 2) time ago. In this regard, the present embodiment has an advantage over the second embodiment which generates data loss corresponding to the time period T1 at least.

【0095】

Further, in the present embodiment, storing of log data in the storage volume 64 is useful also for detection of an computer fraud. Sometimes, crackers (intruders) alter the log data to delete traces of illegal access. In the present embodiment, the replicated volumes 67 can retain snapshots of log data at ΔT' time intervals. For example, a log alteration detection program may be stored in the data protection apparatus 70, the host 40, another computer, the controller 63, or the like. When executed, the program virtually realizes a log alteration detection unit for detecting alteration of log data by comparing respective log data stored in the replicated volumes. Thus, it is possible to monitor an computer fraud against the host 40. Namely, when the log alteration detection unit detects an alteration of the log, and the log alteration detection unit notifies the computer fraud receiving program 73 of the alteration, data of the storage volume used by the host 40 can be protected. In addition, by analyzing snapshots of the log data stored in the replicated volumes, it becomes possible to specify a cracker trying to intrude again, or to take measures such as waylaying.

【0096】

【Effect of the Invention】

As described above, according to the present invention, it is possible to protect data of a computer system at the time of detecting an computer fraud against the computer system.

【Brief Description of the Drawings】

【Fig.1】

Fig. 1 is a cross-sectional view of an LOC (lead on chip) type resin-encapsulated semiconductor apparatus.

【Fig.2】

Fig. 2 is a sequence diagram showing a process flow from an occurrence of an computer fraud against a host 40 to a protection of data in a storage volume 64 in the first embodiment;

【Fig.3】

Fig. 3 is a diagram showing an example of a zoning table 100 held by a switch 50 in the first embodiment;

【Fig.4】

Fig. 4 is a diagram showing an example of a path configuration table 110 held by a controller 63 in the first embodiment;

【Fig.5】

Fig. 5 is a diagram showing an example of an ACL table 120 held by the controller 63 in the first embodiment;

【Fig.6】

Fig. 6 is a block diagram showing a system configuration of a second embodiment of the present invention;

【Fig.7】

Fig. 7 is a block diagram showing a system configuration of a third embodiment of the present invention;

【Fig.8】

Fig. 8 is a sequence diagram showing a processing flow for switching replicated volumes 67a – 67c as destinations of replication of a storage volume 64 in the third embodiment; and

【Fig.9】

Fig. 9 is a diagram showing an cascade example of replicated volumes in the third embodiment.

【Explanation of the Symbols】

10	Computer
20	Network
30	(Front end) Switch
40	Host
43	Intrusion detection program
44	Virus detection software
50	(Back end) Switch
60	Storage apparatus
62	SVP
63	Controller
64	Storage area
66	Transfer delay unit
67	Duplication area
70	Data protection apparatus
73	Illegal act reception program
74	Data protection program
100	Zoning table
110	Path configuration table

120 ACL table

2003-154870

【Document】 Abstract

【Abstract】

【Subject】

When an computer fraud against a computer system is detected, data of the computer system is protected.

【Solution】

A data protection apparatus protects data in a storage volume in a computer system comprising the storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, and a storage control unit for controlling communication between the computer and the storage volume. The data protection apparatus comprises an event detection unit for detecting an event occurrence, and a path disconnection unit for instructing the storage control unit to stop communication between the computer and the storage volume.

【Selected Drawing】 FIG. 1

2003-154870

FIG.1

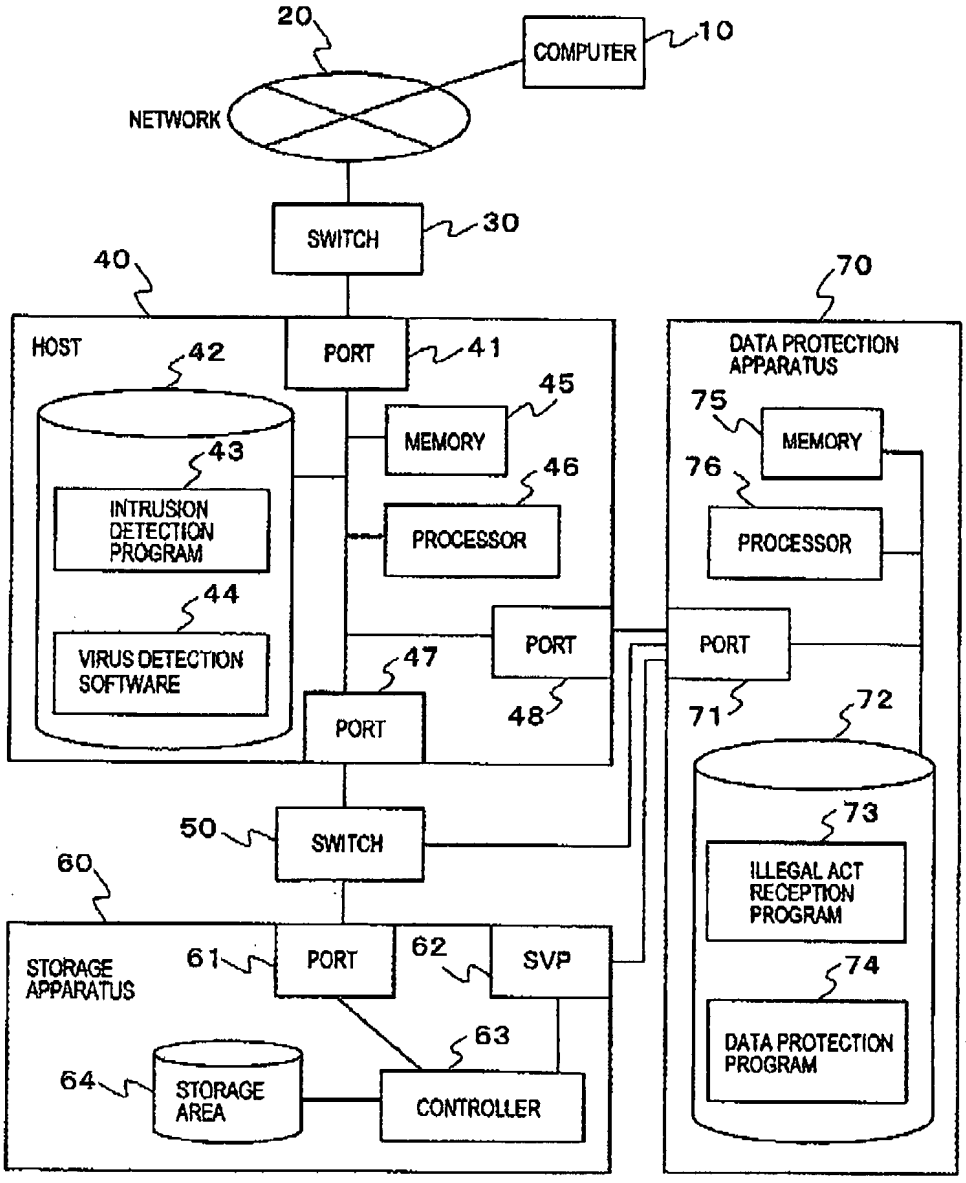

20
COMPUTER
10
NETWORK
SWITCH
30
40
70
HOST
42
PORT
41
DATA PROTECTION APPARATUS
45
75
MEMORY
MEMORY
43
46
76
INTRUSION DETECTION PROGRAM
PROCESSOR
PROCESSOR
44
PORT
PORT
VIRUS DETECTION SOFTWARE
47
48
71
72
PORT
50
SWITCH
73
60
ILLEGAL ACT RECEPTION PROGRAM
STORAGE APPARATUS
61
PORT
62
SVP
74
DATA PROTECTION PROGRAM
63
64
STORAGE AREA
CONTROLLER

FIG.2

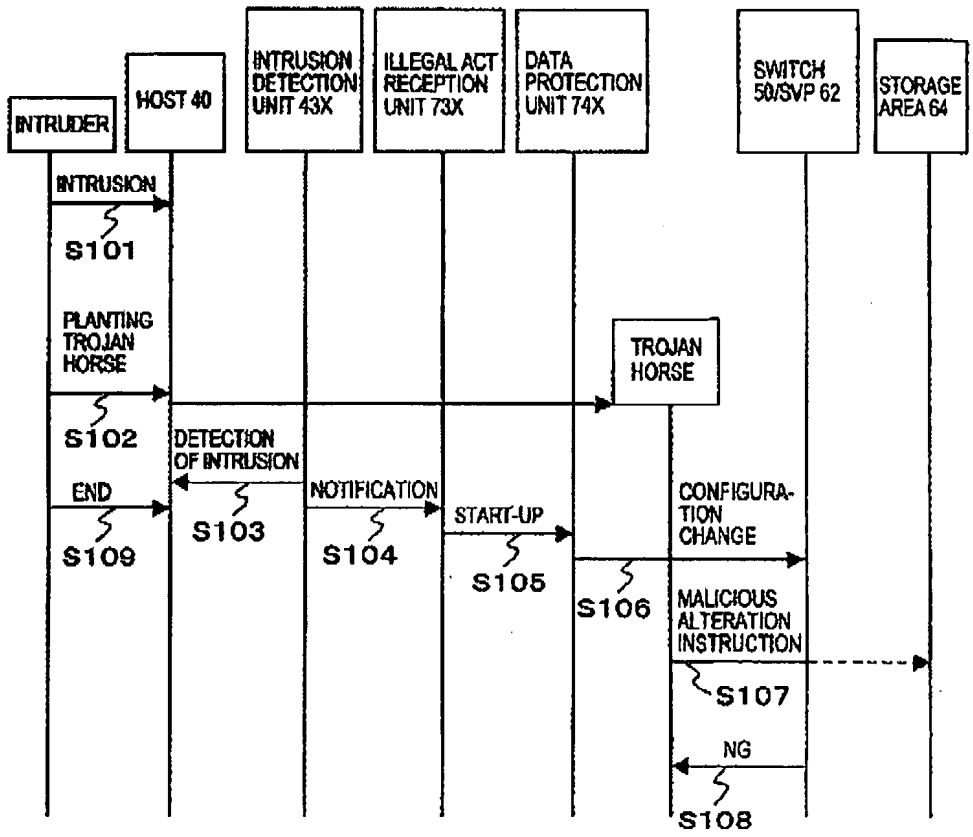

INTRUDER
HOST 40
INTRUSION DETECTION UNIT 43X
ILLEGAL ACT RECEPTION UNIT 73X
DATA PROTECTION UNIT 74X
SWITCH 50/SVP 62
STORAGE AREA 64
INTRUSION
S101
PLANTING TROJAN HORSE
S102
TROJAN HORSE
DETECTION OF INTRUSION
S103
NOTIFICATION
S104
START-UP
S105
S106
CONFIGURA-TION CHANGE
END
S109
MALICIOUS ALTERATION INSTRUCTION
S107
NG
S108

FIG.3

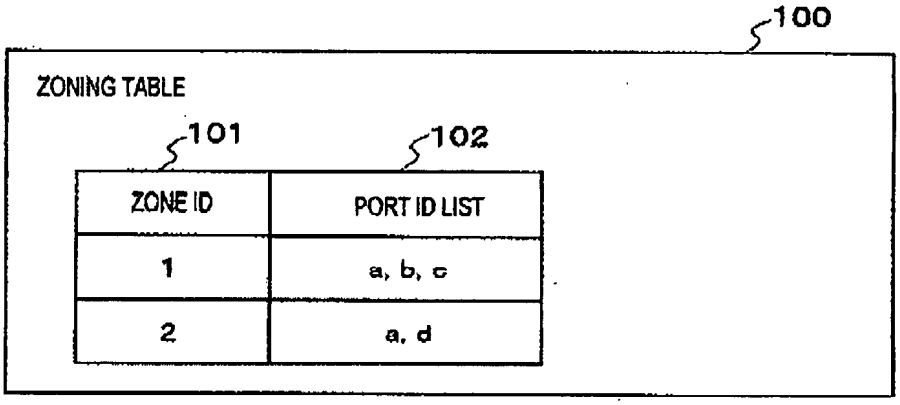

100
ZONING TABLE
101
102
ZONE ID
PORT ID LIST
1
a, b, c
2
a, d

FIG.4

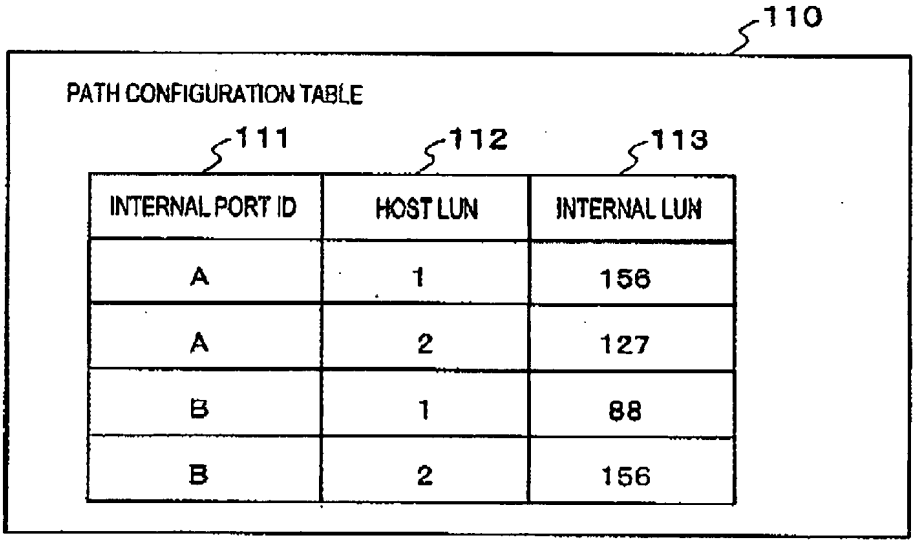

110
PATH CONFIGURATION TABLE
111
112
113
INTERNAL PORT ID
HOST LUN
INTERNAL LUN
A
1
156
A
2
127
B
1
88
B
2
156

FIG.5

120

ACL TABLE

121 INTERNAL PORT ID	122 HOST LUN	123 HOST PORT ID LIST
A	1	a, b, c
A	2	a, d, e
B	1	d, e
B	2	b, c

FIG.6

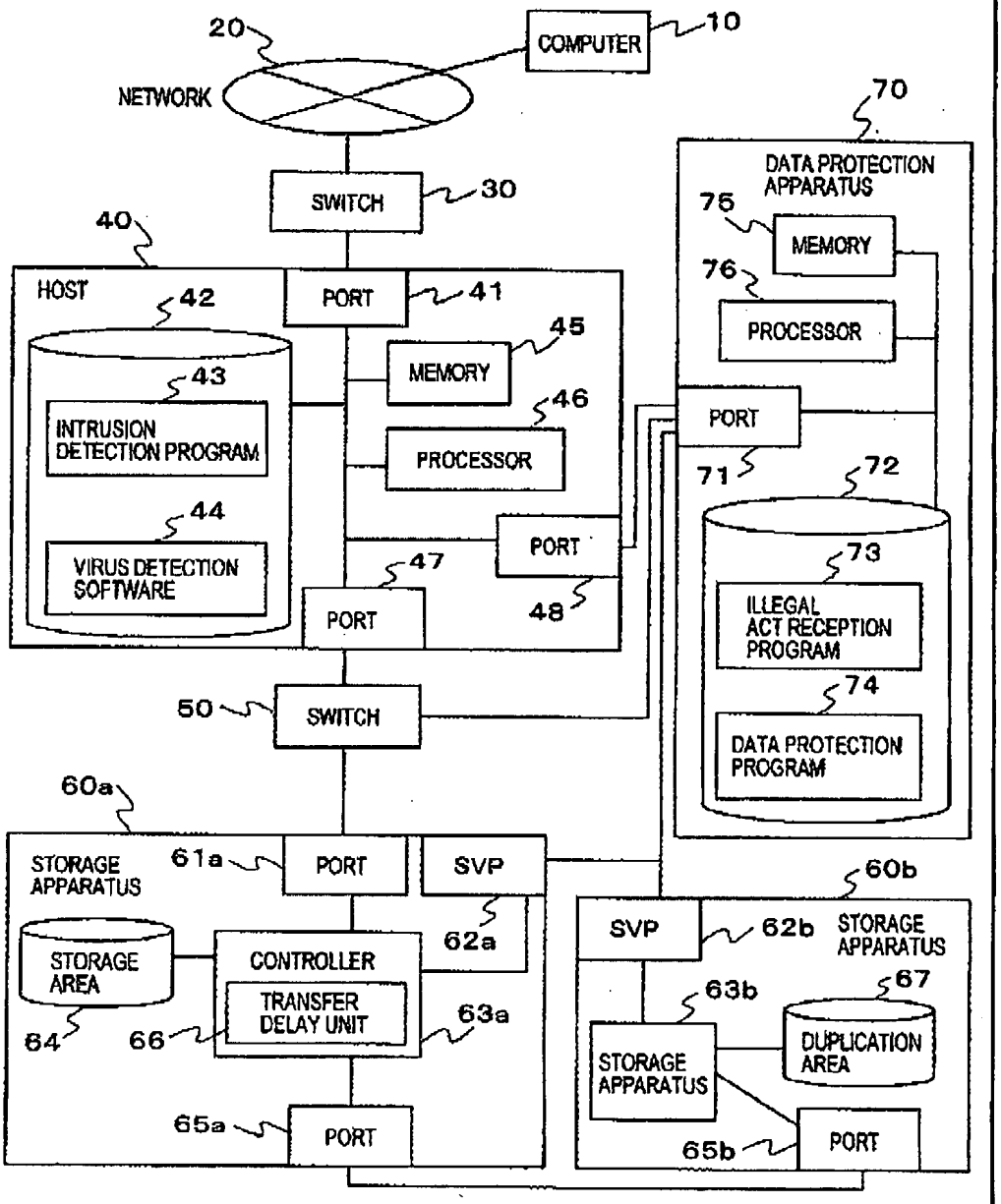

20
NETWORK
COMPUTER
10
70
DATA PROTECTION APPARATUS
75
MEMORY
76
PROCESSOR
SWITCH
30
40
HOST
42
PORT
41
45
MEMORY
43
INTRUSION DETECTION PROGRAM
46
PROCESSOR
PORT
71
72
44
VIRUS DETECTION SOFTWARE
PORT
47
48
PORT
73
ILLEGAL ACT RECEPTION PROGRAM
74
DATA PROTECTION PROGRAM
50
SWITCH
60a
STORAGE APPARATUS
61a
PORT
SVP
60b
62a
SVP
62b
STORAGE APPARATUS
STORAGE AREA
CONTROLLER
TRANSFER DELAY UNIT
63b
67
63a
64
66
STORAGE APPARATUS
DUPLICATION AREA
65a
PORT
65b
PORT

FIG.7

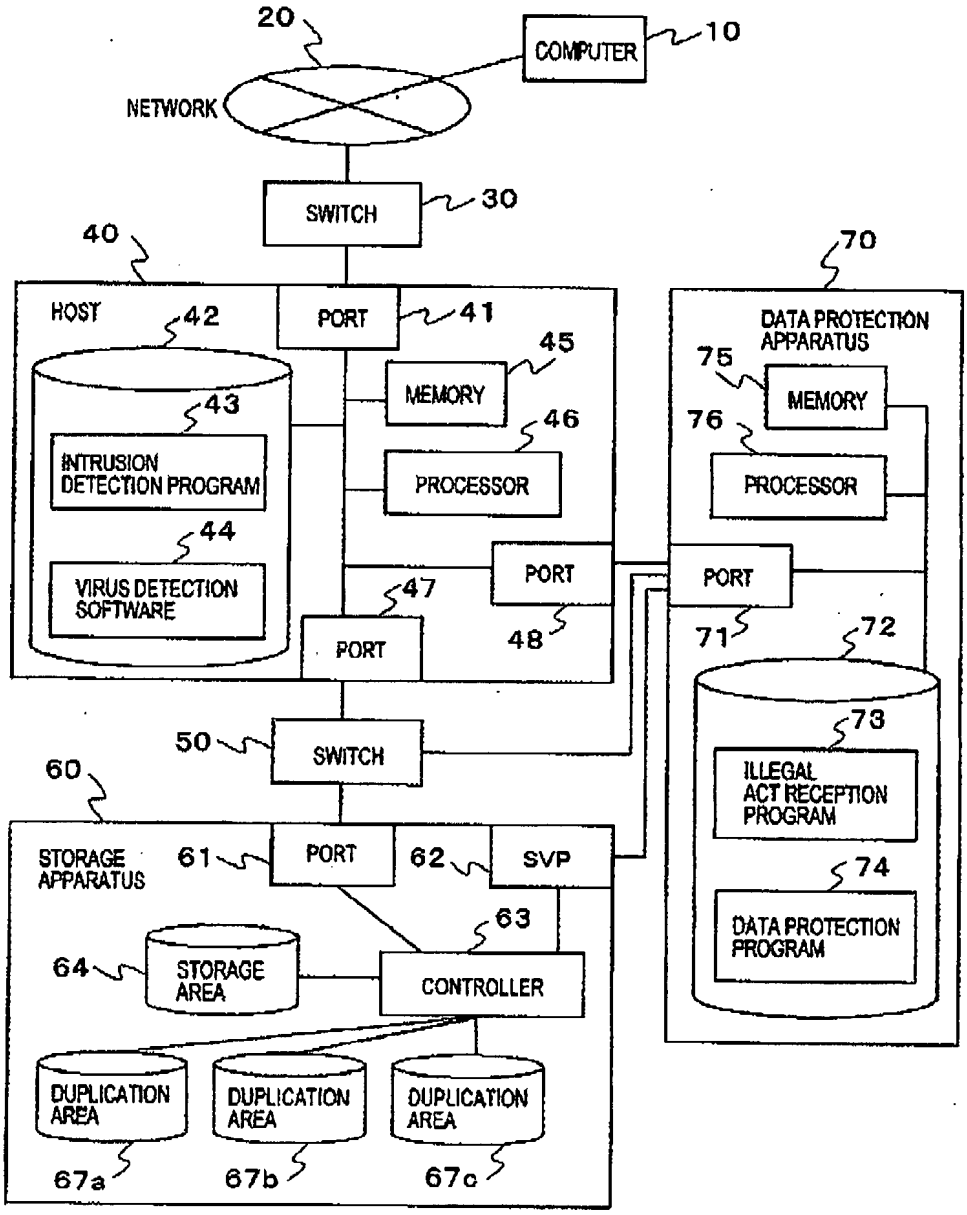

20
NETWORK
COMPUTER
10
SWITCH
30
40
HOST
42
PORT
41
45
MEMORY
43
INTRUSION DETECTION PROGRAM
46
PROCESSOR
44
VIRUS DETECTION SOFTWARE
47
PORT
48
PORT
70
DATA PROTECTION APPARATUS
75
MEMORY
76
PROCESSOR
PORT
71
72
73
ILLEGAL ACT RECEPTION PROGRAM
74
DATA PROTECTION PROGRAM
50
SWITCH
60
STORAGE APPARATUS
61
PORT
62
SVP
63
64
STORAGE AREA
CONTROLLER
DUPLICATION AREA
DUPLICATION AREA
DUPLICATION AREA
67a
67b
67c

FIG.8

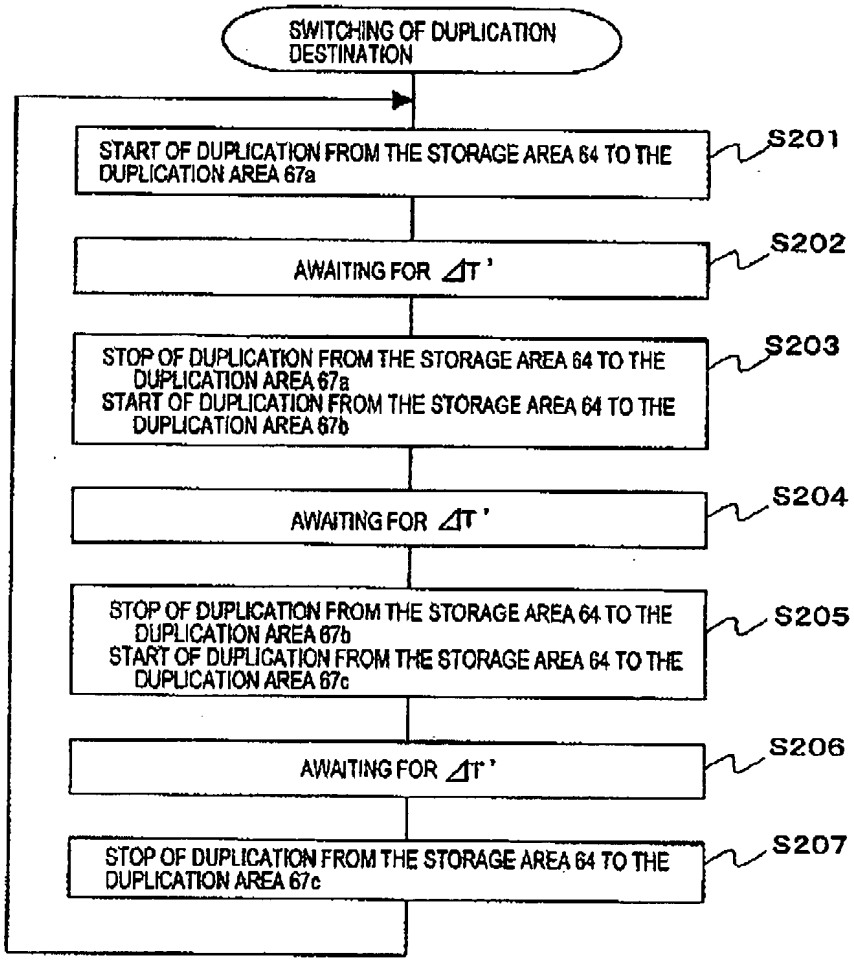
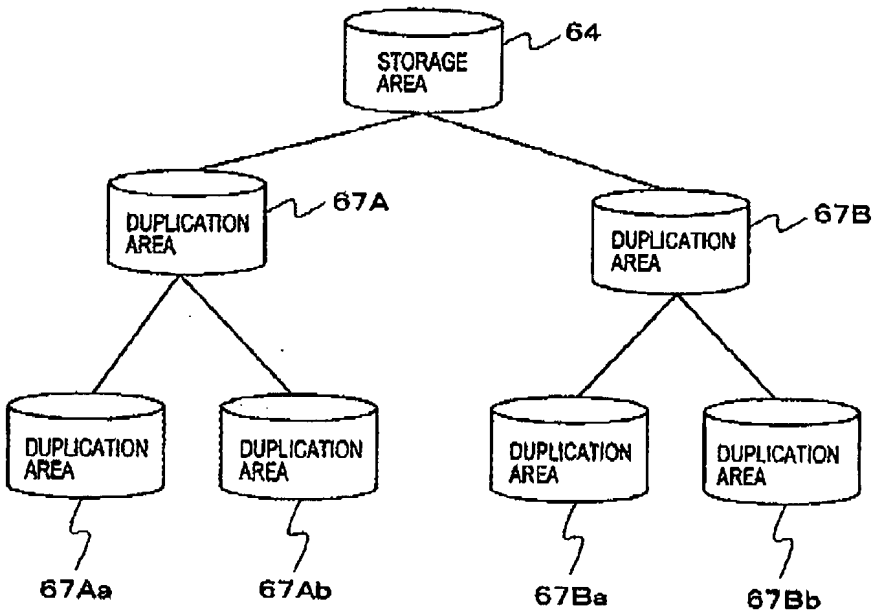

SWITCHING OF DUPLICATION DESTINATION
START OF DUPLICATION FROM THE STORAGE AREA 64 TO THE DUPLICATION AREA 67a
S201
AWAITING FOR ΔT'
S202
STOP OF DUPLICATION FROM THE STORAGE AREA 64 TO THE DUPLICATION AREA 67a
START OF DUPLICATION FROM THE STORAGE AREA 64 TO THE DUPLICATION AREA 67b
S203
AWAITING FOR ΔT'
S204
STOP OF DUPLICATION FROM THE STORAGE AREA 64 TO THE DUPLICATION AREA 67b
START OF DUPLICATION FROM THE STORAGE AREA 64 TO THE DUPLICATION AREA 67c
S205
AWAITING FOR ΔT'
S206
STOP OF DUPLICATION FROM THE STORAGE AREA 64 TO THE DUPLICATION AREA 67c
S207

FIG.9


STORAGE AREA
64
DUPLICATION AREA
67A
DUPLICATION AREA
67B
DUPLICATION AREA
DUPLICATION AREA
DUPLICATION AREA
DUPLICATION AREA
67Aa
67Ab
67Ba
67Bb